



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,954	09/03/2004	Alexander Shipp	117-512	1417

23117 7590 12/11/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER

RAYYAN, SUSAN F

ART UNIT PAPER NUMBER

2167

DATE MAILED: 12/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/500,954

Applicant(s)

SHIPP, ALEXANDER

Examiner

Susan F. Rayyan

Art Unit

2167

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 September 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,5-8 and 11-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-2,5-8,11-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 September 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Response to Arguments

1. Applicant's arguments filed September 18, 2006 have been fully considered but they are not persuasive.

Response to Applicants' arguments concerning the rejection of claims 1-12 under 35 U.S.C. 101 as directed to non-statutory subject matter. Applicant argues in the response on page 10-11 that the signal allows the system (or user) to decide on how the file is subsequently handled and to select the subsequent processing of the file to which they relate. This is very much a real world result. In response to applicants' argument, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Claims 1, 7 would provide a tangible result if the determination of the file to being malware, not malware or unknown, was displayed to the user or stored and retrieved for use at a latter point in time. This would provide the "tangible" (real world) result. Examiner maintains the rejection of claims under 35 U.S.C. 101 as directed to non-statutory subject matter.

Applicant argues on page 14, "the recognition required by the claims 1 and 7 involves determining whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances. This is different than Roberts (paragraph 34) which considers only the internet address, that is the location of the web page and does not consider the contents of the web page. Examiner respectfully disagrees. Roberts' teaches a checksum of the Internet web pages that are

Art Unit: 2167

pre-emptively scanned and stores the URL and checksum (characteristic signature) in the database (paragraph 37) for comparison of the file being processed. The file being processed is first compared to the URL and then to the checksum.

Applicant argues on page 14 of the amendment that Roberts does not teach "records of known executable programs" and "at least one characteristic associated with each instance". Examiner respectfully disagrees. Roberts teaches on paragraph 14 "The malware being scanned for could take a wide variety on form. However, preferred embodiments of the invention seek to detect one or more computer viruses, worms, Trojans, banned computer programs, banned words or banned images" and in paragraph 28 Roberts teaches "internet addresses contain malware (such as the webpage on the internet server". Roberts teaches the detection of a variety of malware which would include detecting these viruses in known executable program. Roberts also teaches malware detected on web pages. Roberts teaches the "database of records of known executable programs" at paragraph 34, lines 1-7 (database storing the internet address that has been pre-emptively scanned for malware and determined to not contain malware). With regard to "at least one characteristic associated with each instance" teaches this limitation at paragraph 37 as storing a checksum associated with the Internet address.

DETAILED ACTION

2. Claims 1-2, 5-8,11-16 are pending.
3. Claims 3-4,9-10 have been canceled.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-2, 5-8,11-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

MPEP 2106 IV.B.2. (b) A claim that requires one or more acts to be performed defines a process. However, not all processes are statutory under 35 U.S.C. 101. Schrader, 22 F.3d at 296, 30 USPQ2d at 1460. To be statutory, a claimed computer-related process must either: (A) result in a physical transformation outside the computer for which a practical application is either disclosed in the specification or would have been known to a skilled artisan, or (B) be limited to a practical application.

Claims 1, 7,13 in view of the above cited MPEP sections, are not statutory because they merely recite a number of computing steps without producing any tangible result and/or being limited to a practical application.

Claim 1 teaches " a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs...", "means for processing a file being transferred between computers ..." and " a difference checker ...", and "means for signaling the file ...". Claims 1 does not would provide a

Art Unit: 2167

real world result such as, displaying to the user or storing to be retrieved and used at a latter point in time the determination of the file to being malware, not malware or unknown. This would provide the “tangible” result.

Claim 7 teaches “maintaining a computer a database containing records of known executable programs ...”, “processing a file ...”, “determining whether the file ...”, “checking, in the case ...”, signaling the file ...” Claims 7 does not would provide a real world result such as, displaying to the user or storing to be retrieved and used at a latter point in time the determination of the file to being malware, not malware or unknown. This would provide the “tangible” result.

Claim 13, teaches “a computer database containing records of known executable programs ...”, “a processor for processing a file ...”, “a processor, depending on the determination ...”. Claims 13 does not would provide a real world result such as, displaying to the user or storing to be retrieved and used at a latter point in time the determination of the file to being malware, not malware or unknown. This would provide the “tangible” result.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2, 5-8, 11-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "likely" in claims 1, 7, 13, 16 is a relative term which renders the claim indefinite. The term "likely" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term likely is unclear as to whether the file has been determined to be malware or not.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 7-11, 13-15 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication Number 2004/0088570 issued to Guy William Welch Roberts et al ("Roberts").

Art Unit: 2167

As per claims 1,7 Roberts anticipates:

a) a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be

determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each instance (see paragraph 34, lines 1-7 and paragraph 37 as storing a checksum associated with the internet address.);

b) means for processing a file being transferred between computers , the means comprising : a file recognizer operative for determine whether the file being processed is an instance of a known file being processed for the presence of said at least one characteristic signature associated with the said instances (paragraph 36, lines 6-10, paragraph 37, lines 1-3 and Figure 6, Ref. No. 42 and paragraph 37, lines 8-13, compare checksum against new checksum);

a difference checker operative , in the case that the file recognizer determines the file being processed to be an instance of a known program to check whether the file is an unchanged version of that known program (paragraph 37, lines 8-14, checksum);

and c) means for signaling the file depending on the determination made by the processing means , as being :

likely to be not malware if it is an unchanged version of a known file, likely to be malware if it is a changed version of a known file, or of unknown status if it is not determined as being an instance of a known file (paragraph 38, lines 1-12).

Art Unit: 2167

Claim 7 is rejected based on the same rationale as independent claim 1.

As per claims 2, 8, same as claim arguments above and Roberts anticipates:

d) means for processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware and wherein the means d) is operative to subject a file to processing if the file signaled by the signaling means c) as being of unknown status (paragraph 37, lines 1-6 and paragraph 38).

As per claims 5, 11, same as claim arguments above and Roberts anticipates:

wherein the difference checker is operative to generate a checksum for the entire file under consideration or for at least one selected region thereof, and to compare the checksum or checksums with those of entries in the database (paragraph 37, lines 8-14).

Claim 13 is rejected based on the same rationale as independent claim 1.

Claim 14 is rejected based on the same rationale as claims above and Roberts anticipates:

a file scanning subsystem for scanning files identified by the processor as being of unknown status to determine whether the scanned files are malware (paragraph 38 lines 4-6, content has change (checksum does not match) so it is unknown if the change is due to malware and it is rescanned).

Art Unit: 2167

Claim 15, same as claim arguments above and Roberts anticipates:

wherein the records for files which are instances of programs determined by the file-scanning system not to be malware are added to the computer database(see paragraph 34, lines 1-7).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6,12 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication Number 2004/0088570 issued to Guy William Welch Roberts et al ("Roberts") in view of US Patent Number 5,617,533 issued to Wu et al ("Wu").

As per claim 6, 12 Roberts teaches signaling means is operative to signal the file as malware ... or as unknown if it is (paragraph 38). Roberts does not explicitly teach including an exception list handler for determining, in relation to a file which the processing means b) has determined is not a known file, whether that file has characteristics matching an entry in an exception list of files. Wu does teach these limitations at column 8, lines 7-17, column 12, lines 54-60 and column 13, lines 32-45. It

Art Unit: 2167

would have been obvious to one of ordinary skill in the art at the time of the invention to combine the cited references to determine whether the corresponding software conforms with package rules (column 7, lines 50-57).

8. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication Number 2004/0088570 issued to Guy William Welch Roberts et al ("Roberts") in view of US Patent Application 2004/0128355 issued to Chao et al ("Chao").

Claim 16, same as claim arguments above and Roberts does not explicitly teach wherein the processor assigns a score to a file identified as likely to be malware. Chao does teach this limitation (paragraph 34, lines 3-10 and paragraph 25, lines 12-21 as virus classification score) to provide the user with a warning message that an executable has been deleted due to a virus. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Roberts with wherein the processor assigns a score to a file identified as likely to be malware to provide the user with a warning message that an executable has been deleted due to a virus (paragraph 37, lines 13-21).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Susan Rayyan whose telephone number is (571) 272-1675. The examiner can normally be reached M-F: 8am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on (571) 272-7079. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

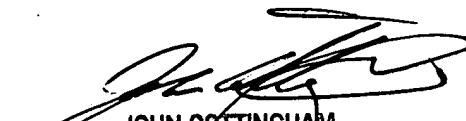
Art Unit: 2167

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Susan Rayyan

December 1, 2006



JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100